REMARKS

Initially, in the Office Action dated February 10, 2004, the Examiner rejects claims 3 and 4 under 35 U.S.C. §112, second paragraph. Claim 12 and 13 are objected to as containing duplicate information. Claim 23 is objected to because of informalities. Claims 1 and 24 have been rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,385,729 (DiGiorgio et al.) in view of U.S. Patent No. 6,516,316 (Ramasubramani et al.). Claims 2 and 7 have been rejected under 35 U.S.C. §103(a) as being unpatentable over DiGiorgio et al. and Ramasubramani et al. in view of U.S. Patent No. 6,026,472 (Cheung). Claims 9 and 10 have been rejected under 35 U.S.C. §103(a) as being unpatentable over DiGiorgio et al. and Ramasubramani et al. and further in view of U.S. Patent No. 6,285,991 (Powar). Claim 11 has been rejected under 35 U.S.C. §103(a) as being unpatentable over DiGiorgio et al., Ramasubramani et al. and Powar and further in view of International Publication No. WO 99/49404 (Cochinwala et al.). Claims 14, 15, 19 and 20 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Ramasubramani et al. and Cheung in view of DiGiorgio et al. Claims 16 and 17 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Ramasubramani et al., Cheung and DiGiorgio et al. and further in view of Cochinwala et al. Claim 18 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Ramasubramani et al., Cheung and DiGiorgio et al. in view of "The GSM System" (Mouly et al.). Claims 21-23 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Ramasubramani et al. and Cheung in

view of DiGiorgio et al. and further in view of Cochinwala et al. Claims 5, 6 and 8 have been objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

By the present response, Applicants have canceled claims 12 and 13 without disclaimer. Applicants have amended claims 1, 3 and 23 to further clarify the invention and added new claim 25. Claims 1-11, 14-25 remain pending in the present application.

Allowable Subject Matter

Applicants thank the Examiner for indicating that claims 5, 6 and 8 contain allowable subject matter.

35 U.S.C. §112 Rejections

Claims 3 and 4 have been rejected under 35 U.S.C. §112, second paragraph. Applicants have amended these claims to further clarify the invention and respectfully request that these rejections be withdrawn.

Claim Objections

Claims 12, 13 and 23 have been objected to because of informalities. Claims 12 and 13 have been canceled. Claim 23 has been amended to further clarify the invention. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

35 U.S.C. §103 Rejections

Claims 1 and 24 have been rejected under 35 U.S.C. §103(a) as being unpatentable over DiGiorgio et al. in view of Ramasubramani et al. Applicants respectfully traverse these rejections.

DiGiorgio et al. discloses a secure token device such as a smart card or an ibutton that provides a user with a vehicle for accessing services that are provided by an Internet service provider (ISP). The user places the secure token device in communication with a reader that is coupled to a computer system that includes a web browser for accessing the services provided by the ISP. The secure token device may perform an authentication protocol to authenticate itself to the ISP. The ISP may also be required to authenticate itself. The secure token device may hold an electronic currency token for payment of services rendered by the ISP.

Ramasubramani et al. discloses a centralized certificate management system for thin client in data networks. This may be used in systems having a large number of the thin clients serviced by a proxy server through which the thin clients communicate with a plurality of secure server computers over a data network. A certificate management module causes the server device to manage digital certificates for each of the thin client devices. Computing resources in a server device is used to carry out the task of obtaining and maintaining certificates asynchronously in the proxy server and further.

Applicants submit that neither DiGiorgio et al. nor Ramasubramani et al., taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 1, 24 and new claim 25 of, inter alia,

verifying the identity of a mobile station by a gateway by accessing an authentication center of a cellular network and comparing mobile station generated variables computed by the mobile station with gateway generated variables computed by the gateway, verifying the legitimacy of the gateway by the mobile station by comparing the variables computed by the gateway with the variables computed by the mobile station, requesting a digital certificate by the mobile station from the gateway used to order and authorize a product or service from a service provider, delivering a digital certificate to the mobile station by the gateway when the identity of the mobile station has been verified, or transmitting a digital signature by the mobile station accompanied by the digital certificate for a signature verification key as authorization to the service provider. The Examiner asserts that DiGiorgio et al. discloses verifying the identity of a mobile station by a gateway and verifying the legitimacy of a gateway at col. 10, lines 24-60 and col. 5, line 47. However, this portion of DiGiorgio et al. merely discloses a two-way challenge response authentication process between an ISP at a remote server and a secure token device where each issues a challenge to the other to authenticate each other. This is not verifying the identity of a mobile station by a gateway by accessing an authentication center of a cellular network, as recited in the claims of the present application. DiGiorgio et al. discloses authentication between a secure token device at a computer and an ISP at a remote server. DiGiorgio et al. does not disclose or suggest an authentication center of a cellular network, or this authentication center being accessed by a gateway to verify the identity of a mobile station.

DiGiorgio et al. discloses a secure token kind of feature where token can be used for identifying the token owner for storing contextual information, support electronic payments by transferring payments from the token to an ISP and for storing personal information of the user. The token can be used for setting up the parameters for the connection session on behalf of a user manually. DiGiorgio et al. does not disclose or suggest a cellular network authentication center, or a digital certificate and signature being used, or a gateway.

The Examiner admits that DiGiorgio et al. does not disclose or suggest several limitations in the claims of the present application such as the gateway accessing an authentication center, requesting a digital certificate by the mobile station from the gateway used to order and authorize a product or service from a service provider, delivering a digital certificate to the mobile station by the gateway when the identity of the mobile station had been verified, requesting a product or service from the service provider, or transmitting a digital signature by the mobile station accompanied by the digital certificate for a signature verification key as authorization to the service provider, but asserts that Ramasubramani et al. discloses these limitations at col. 8, lines 41-48, col. 9, lines 45-54, col. 11, lines 37-41 and col. 4, lines 25-34. However, these portions of Ramasubramani et al. merely disclose accessing an account of a device in a proxy server by depressing a key to send a request that includes a URL to the proxy server, a gateway receiving a user name and password and comparing them with ones in the account and providing access to the account based on a match, a CA receiving a certificate request and

verifying the supplied information to validate a user's public key along with other information and signing a certificate and then issuing a certificate response containing the signed certificate or an error, and digital IDs between a client and a merchant server where a user sends messages to a merchant website by signing the messages and enclosing his digital ID to ensure the recipient of the message that the message was actually sent by him. These portions of Ramasubramani et al. do not disclose or suggest anything related to an authentication center of a cellular network that is accessed by a gateway to verify the identity of a mobile station, as recited in the claims of the present application. Moreover, these portions of Ramasubramani et al. do not disclose or suggest a gateway as used and recited in the claims of the present application. According to the present invention, a gateway is accessed by a mobile station and the gateway accesses an authentication center of a cellular network. Further, the legitimacy of the gateway is verified by a mobile station, and the mobile station requests a digital certificate from the gateway to be used to order and authorize a product or service from a service provider. Ramasubramani et al. merely discloses managing centralized certificates, and how to access a secure server from the client devices using a certificate allocated to certain client device. A server in Ramasubramani et al. is not a gateway, as recited in the claims of the present application. A gateway generally sits between two networks and/or devices—as in the present claims the gateway is connected to both a mobile station and an authentication center. Further, as noted previously,

Ramasubramani et al. does not disclose or suggest a cellular network authentication center as recited in the claims of the present application

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 1, 24 and 25 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 2 and 7 have been rejected under 35 U.S.C. §103(a) as being unpatentable over DiGiorgio et al., Ramasubramani et al. and further in view of Cheung. Applicants have discussed the deficiencies of Cheung in Applicants' previously-filed response. Applicants respectfully traverse these rejections and submit that claims 2 and 7 are dependent on independent claim 1 and, therefore, are patentable at least for the same reasons noted regarding this independent claim. Cheung does not overcome the substantial defects noted previously regarding DiGiorgio et al. and Ramasubramani et al. For example, none of the cited references disclose or suggest transmitting in at least one message a signed response, a public key and a variable M2 computed by the mobile station to the gateway computing a variable M2' by the gateway, or verifying the identify of the mobile station when the variable M2 is equal to the variable M2'.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 2 and 7 of the present application. Applicants

respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 9 and 10 have been rejected under 35 U.S.C. §103(a) as being unpatentable over DiGiorgio et al., Ramasubramani et al. and further in view of Powar. Applicants have discussed the deficiencies of Powar in Applicants' previously-filed response. Applicants submit that claims 9 and 10 are dependent on independent claim 1 and, therefore, are patentable at least for the same reasons noted regarding this independent claim. Powar does not overcome the substantial defects noted previously regarding DiGiorgio et al. and Ramasubramani et al. For example, Applicants submit that none of the cited references disclose or suggest verifying that restrictions associated with the digital certificate are not violated or creating an accounting record for the product or service sold.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 9 and 10 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claim 11 has been rejected under 35 U.S.C. §103(a) as being unpatentable over DiGiorgio et al., Ramasubramani et al., Powar and further in view of Cochinwala et al. Applicants have discussed the deficiencies of Cochinwala et al. in Applicants' previously-filed response. Applicants submit that claim 11 is dependent on independent claim 1 and, therefore, is patentable at least for the same reasons

noted regarding this independent claim. Neither Powar nor Cochinwala et al. overcome the substantial defects noted previously regarding DiGiorgio et al. and Ramasubramani et al. For example, Applicants submit that none of the cited references disclose or suggest transmitting from the service provider to the gateway the accounting record having an invoice and digital signature of a customer of a home network operator service, or crediting the service provider with an amount equal to that in the invoice and billing the buyer with the amount of the invoice.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of claim 11 of the present application. Applicants respectfully request that this rejection be withdrawn and that this claim be allowed.

Claims 14, 15, 19 and 20 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Ramasubramani et al., Cheung in view of DiGiorgio et al. Applicants respectfully traverse these rejections.

Regarding claims 14 and 19, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of these claims of, inter alia, [insert limitations from above]

Regarding claims 15 and 20, Applicants submit that these claims are dependent on one of independent claims 14 and 19 and, therefore, are patentable at least for the same reasons noted regarding these independent claims. Applicants submit that Cheung does not overcome the substantial defects noted previously

regarding Ramasubramani et al. and DiGiorgio et al. For example, none of the cited references disclose or suggest where the mobile station certificate acquisition module verifies that the gateway is authorized to issue the digital certificate through the use of comparing variables computed by the gateway and the mobile station.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 14, 15, 19 and 20 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 16 and 17 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Ramasubramani et al., Cheung, DiGiorgio et al. and further in view of Cochinwala et al. Applicants have discussed the deficiencies of Cochinwala et al. in Applicants' previously-filed response. Applicants respectfully traverse these rejections and submit that claims 16 and 17 are dependent on independent claim 14 and, therefore, are patentable at least for the same reasons noted regarding this independent claim. Applicants submit that neither Cheung nor Cochinwala et al. overcome the substantial defects noted previously regarding Ramasubramani et al. and DiGiorgio et al. For example, none of the cited references disclose or suggest where the gateway certificate generation module transmits a mobile subscriber identifier to the authentication center, receives a random number, a signed response and an encryption key from the authentication center, computes a variable M1, M2', and M3 and verifies the validity of the mobile

station by comparing variable M2 received from the mobile station with variable M2'. Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 16 and 17 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claim 18 has been rejected under 35 U.S.C. §103(a) as being unpatentable over Ramasubramani et al., Cheung, DiGiorgio et al. and further in view of Mouly et al. Applicants have discussed the deficiencies of Mouly et al. in Applicants' previously-filed response. Applicants respectfully traverse these rejections and submit that claim 18 is dependent on independent claim 14 and, therefore, is patentable at least for the same reasons noted regarding this independent claim. Neither Cheung nor Mouly et al. overcome the substantial defects noted previously regarding Ramasubramani et al. and DiGiorgio et al. For example, Applicants submit that none of the cited references disclose or suggest a subscriber identification module used to compute a signed response and a ciphering key based on a secret key, installed by a home network operator service in the subscriber identification module upon signing up for a service plan or an A3 algorithm module or an A8 algorithm module.

Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in

the combination of claim 18 of the present application. Applicants respectfully request that this rejection be withdrawn and that this claim be allowed.

Claims 21-23 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Ramasubramani et al., Cheung, DiGiorgio et al. and further in view of Cochinwala et al. Applicants respectfully traverse these rejections and submit that claims 21-23 are dependent on independent claim 19 and, therefore, are patentable at least for the same reasons noted regarding this independent claim. Neither Cheung nor Cochinwala et al. overcome the substantial defects noted previously regarding Ramasubramani et al. and DiGiorgio et al. For example, Applicants submit that none of the cited references disclose or suggest where the mobile station certificate acquisition code segment transmits a session identification and a mobile subscriber identifier to the gateway, receives a random number and a variable M1 from the gateway and verifies that the gateway is authentic by computing and comparing the variable M1' with M1.

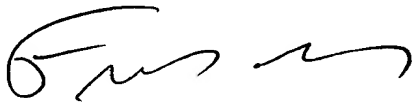
Accordingly, Applicants submit that none of the cited references, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 21-23 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

In view of the foregoing amendments and remarks, Applicants submit that claims 1-11 and 14-25 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135 (referencing attorney docket no. 0173.38633X00).

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Frederick D. Bailey
Registration No. 42,282

FDB/sdb
(703) 312-6600